

Claims

What is claimed is:

1. A method for use in generating digital signatures in an information processing system, the system including at least a user device, an intermediary device and a verifier, the method
5 comprising the steps of:

generating in the user device a first digital signature; and
sending the first digital signature to the verifier;

wherein the verifier sends the first digital signature to the intermediary device, and the intermediary device checks that the first digital signature is a valid digital signature for the user
10 device and if the first digital signature is valid generates a second digital signature which is returned to the verifier as a signature generated by the user device.

2. The method of claim 1 wherein the first digital signature is generated using a first secret key associated with a first digital signature protocol having a computational efficiency compatible with computational resources of the user device.

3. The method of claim 2 wherein the second digital signature is generated using a second secret key associated with second digital signature protocol having a computational efficiency lower than that of the first digital signature protocol.

4. The method of claim 3 wherein an agreement relating to corresponding public keys of the first and second digital signature protocols is signed by both the user device and the intermediary device and the resulting twice-signed agreement is stored by both the user device and the intermediary device.

5. The method of claim 3 wherein the second secret key associated with the second digital signature protocol is supplied from the user device to the intermediary device over a secure private channel.

6. The method of claim 1 wherein the first digital signature comprises a signature s_1 on a message m , the signature s_1 being generated using a secret key s' of a key pair (s', p') associated with the user device.

5 7. The method of claim 1 wherein the first digital signature comprises a signature s_1 on $h(m)$, where m is a message and h is a hash function, the signature s_1 being generated using a secret key s' of a key pair (s', p') associated with the user device.

10 8. The method of claim 3 wherein the verifier upon receipt of the first digital signature checks that the first digital signature is a valid digital signature using a first public key corresponding to the first secret key.

15 9. The method of claim 1 wherein the second digital signature comprises a signature s_2 on a message m , the signature s_2 being generated using a secret key s of a key pair (s, p) associated with the user device.

20 10. The method of claim 1 wherein the second digital signature comprises a signature s_2 on $h(m)$, where m is a message and h is a hash function, the signature s_2 being generated using a secret key s of a key pair (s, p) associated with the user device.

25 11. The method of claim 2 wherein the verifier upon receipt of the second digital signature checks that the second digital signature is a valid digital signature using a second public key corresponding to the second secret key.

30 12. The method of claim 1 wherein the user device is switchable between a normal operating mode and a secure operating mode.

35 13. The method of claim 1 wherein the first digital signature is generated only after user verification of the message to be signed.

14. The method of claim 1 wherein at least one of first and second secret keys used to generate the respective first and second and second digital signatures are stored in an at least partially encrypted form on the user device and the intermediary device, respectively.

15. The method of claim 1 wherein at least one of first and second secret keys used to generate the respective first and second and second digital signatures is configured such that a first portion thereof is stored in the user device and a second portion thereof is stored in a storage element removable from the user device.

16. The method of claim 1 wherein if a user associated with the user device can contact the intermediary device and upon providing an access code thereto direct the intermediary device not to generate the second digital signature.

17. The method of claim 1 wherein the intermediary device is configured to wait a predetermined delay period between checking that the first digital signature is a valid signature and generating the second digital signature which is returned to the verifier.

18. The method of claim 1 wherein the user device precomputes a plurality of coupons, a given one of the coupons being utilizable to generate the first digital signature.

19. The method of claim 1 wherein the user device comprises a mobile telephone.

20. The method of claim 1 wherein the user device comprises a personal digital assistant (PDA).

21. The method of claim 1 wherein the user device comprises a wearable computer.

22. An apparatus for use in generating digital signatures in an information processing system, the system including at least a user device, an intermediary device and a verifier, the apparatus comprising:

a memory; and

a processor coupled to the memory, the processor being operative to generate in the user device a first digital signature, and to send the first digital signature to the verifier;

wherein the verifier sends the first digital signature to the intermediary device, and the intermediary device checks that the first digital signature is a valid digital signature for the user device and if the first digital signature is valid generates a second digital signature which is returned to the verifier as a signature generated by the user device.

23. An article of manufacture comprising a machine-readable storage medium for storing one or more programs for use in generating digital signatures in an information processing system, the system including at least a user device, an intermediary device and a verifier, wherein the one or more programs when executed implement the steps of:

generating in the user device a first digital signature; and

sending the first digital signature to the verifier;

wherein the verifier sends the first digital signature to the intermediary device, and the intermediary device checks that the first digital signature is a valid digital signature for the user device and if the first digital signature is valid generates a second digital signature which is returned to the verifier as a signature generated by the user device.

24. A method for use in generating digital signatures in an information processing system, the system including at least a user device, an intermediary device and a verifier, the method comprising the steps of:

receiving in the verifier from the user device a first digital signature; and

sending the first digital signature from the verifier to the intermediary device;

wherein the intermediary device checks that the first digital signature is a valid digital signature for the user device and if the first digital signature is valid generates a second digital signature which is returned to the verifier as a signature generated by the user device.

5 25. A method for use in generating digital signatures in an information processing system, the system including at least a user device, an intermediary device and a verifier, the method comprising the steps of:

 receiving in the intermediary device a first digital signature generated in the user device and sent to the intermediary device from the verifier;

10 checking in the intermediary device that the first digital signature is a valid digital signature for the user device; and

 if the first digital signature is valid generating a second digital signature which is returned to the verifier as a signature generated by the user device.